VÖWG
Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs

VKÖ
Verband kommunaler Unternehmen Österreichs

NISG 2026 und RKEG: Resilienz im Vergaberecht
„Vergabetoolbox“

Über den Verband der öffentlichen Wirtschaft und Gemeinwirtschaft Österreichs

Unser Ziel ist es, dass Dienstleistungen der Daseinsvorsorge für alle Menschen in Österreich zugänglich, leistbar und von hoher Qualität bleiben – heute und in Zukunft. Der VÖWG vernetzt über 120 Unternehmen, Institutionen und Organisationen und fördert den Wissensaustausch – etwa in den Bereichen Energieversorgung, öffentlicher Verkehr, Wasser- und Abwasserwirtschaft, Abfallentsorgung, wirtschafts- und finanzpolitische Steuerung, Wohnen sowie Gesundheits- und Sozialdienste. Zudem unterstützt der VÖWG seine Mitglieder mit einem breiten Serviceangebot, begleitet politische und regulatorische Entwicklungen und stärkt die Stimme der Daseinsvorsorge auf nationaler und europäischer Ebene.

Über den Verband kommunaler Unternehmen Österreichs

Der Verband kommunaler Unternehmen Österreichs (VKÖ) vereint rund 30 kommunale Unternehmen aus ganz Österreich sowie die Stadtwerke Krakau und Meran. Mit ihren breiten Portfolios in den Bereichen Energieversorgung, Netzinfrastruktur, öffentlicher Verkehr, Wasser- und Abwasserwirtschaft, Abfallwirtschaft und Telekommunikation leisten sie einen wesentlichen Beitrag zu einer sicheren und leistbaren Daseinsvorsorge. Der VKÖ unterstützt seine Mitglieder mit vielfältigen Services, begleitet politische und regulatorische Entwicklungen und stärkt die Stimme der kommunalen Daseinsvorsorge auf nationaler und europäischer Ebene.

Rechtsform:
Verein

Sitz:
Stadiongasse 6-8, A-1010 Wien

ZVR-Zahl (AT):
VÖWG: 338965482
VKÖ: 358163335

Zuständigkeit:
Landespolizeidirektion Wien

EU-Transparenzregisternummer VÖWG:
643879152710-58

In Zusammenarbeit mit Heid & Partner Rechtsanwälte (RA Mag. Berthold Hofbauer).

HEID & PARTNER
RECHTSANWÄLTE

1. Einleitung: Worum es in diesem Leitfaden geht

Geopolitische Unsicherheit, hybride Bedrohungen, Cyberangriffe, physische Angriffe auf Infrastruktur, Lieferkettenstörungen und die fortschreitende Digitalisierung haben die Beschaffungspraxis nachhaltig verändert. Öffentliche Auftraggeber, Sektorenauftraggeber und Betreiber kritischer Einrichtungen beschaffen nicht mehr bloß Waren, Bau- oder Dienstleistungen. Sie entscheiden mit jeder sicherheitsrelevanten Vergabe auch darüber, welche Risiken sie in ihre Organisation hineinlassen, welche Abhängigkeiten sie begründen und wie belastbar ihre Betriebs- und Wiederanlaufprozesse im Ernstfall sind.

Die Europäische Union hat auf diese Entwicklungen insbesondere mit der NIS-2-Richtlinie[1] und der RKE-Richtlinie[2] reagiert. In Österreich wurden diese Vorgaben durch das Netz- und Informationssystemsicherheitsgesetz 2026[3] (**„NISG 2026“**) und das Resilienz kritischer Einrichtungen-Gesetz[4] (**„RKEG“**) umgesetzt. Das NISG 2026 ordnet die Anforderungen an die Cybersicherheit von Netz- und Informationssystemen neu. Das RKEG richtet den Blick auf die Widerstandsfähigkeit kritischer Einrichtungen und die Aufrechterhaltung wesentlicher Dienste. Ergänzend zum RKEG ist die Resilienz kritischer Einrichtungen-Verordnung[5] (**„RKEV“**) zu berücksichtigen. Sie konkretisiert insbesondere Schwellenwerte für die Ermittlung kritischer Einrichtungen und für die Beurteilung meldepflichtiger Sicherheitsvorfälle.

Für Beschaffungsvorgänge folgt daraus eine deutliche Verdichtung der Anforderungen. Sicherheits- und Resilienzaspekte sind zwar nicht in jedem Vergabeverfahren verfahrensprägend, sie können aber – je nach Auftraggeber, Leistungsgegenstand, Kritikalität und Einbindung externer Dritter – rechtlich, technisch und/oder organisatorisch geboten sein. Betroffen sind nicht nur große „Hochrisikoprojekte“. In der Praxis entstehen viele Risiken bereits bei scheinbar „gewöhnlichen“ Leistungen, wenn Auftragnehmer Zugang zu Anlagen, Systemen, Daten, Baustellen, Betriebsprozessen oder sonstigen sensiblen Schnittstellen erhalten.

Dieser Leitfaden versteht sich als erste **Orientierungshilfe und Basistoolbox**. Er soll eine erste Verortung ermöglichen, typische Risikokonstellationen sichtbar machen und Standardbausteine bereitstellen, die eine belastbare Mindestabsicherung für „Risikoprojekte“ ermöglichen. Unter „Risikoprojekten“ versteht der Leitfaden dabei typische Beschaffungsvorgänge mit sicherheits-, betriebs- und/oder resilienzrelevanten Schnittstellen, die über ein bloßes „Standardprojekt“ hinausgehen, aber noch keine projektspezifische „Hochrisikobeschaffung“ darstellen. Der Leitfaden ersetzt somit keine allenfalls notwendige projektspezifische Lösung nach Maß: Für komplexe IT-/OT-Systeme, sensible Betriebsanlagen oder international verzweigte Lieferketten ist eine vertiefte rechtliche, technische und organisatorische Einzelprüfung unverzichtbar.

2. Der Leitfaden in zehn Leitsätzen

Der Leitfaden folgt einer einfachen Dramaturgie: Zunächst werden NISG 2026 und RKEG in ihren Grundzügen erklärt. Danach wird gezeigt, weshalb beide Regelungswerke in Beschaffungen hineinwirken. Anschließend wird eine praktische Reiseroute dargestellt: Kritikalität prüfen, Mindestanforderungen im Rahmen der Leistungsbeschreibung festhalten, geeignete Unternehmen auswählen, echte Mehrwerte bewerten und die Leistung vertraglich absichern. Die folgenden Leitsätze fassen diese Logik vorab zusammen:

1. NISG 2026 und RKEG verfolgen zwar unterschiedliche Schutzrichtungen, in der Beschaffungspraxis treffen sie jedoch häufig auf denselben Leistungsgegenstand und ergänzen sich wechselseitig.

2. Das NISG 2026 betrifft die Cybersicherheit von Netz- und Informationssystemen und macht insbesondere Risikomanagement, Lieferkette, Meldeprozesse, Governance und Nachweisführung beschaffungsrelevant.

[1] CELEX-Nr.: 32022L2555.
[2] CELEX-Nr.: 32022L2557.
[3] Bundesgesetz zur Gewährleistung eines hohen Cybersicherheitsniveaus von Netz- und Informationssystemen, BGBl I Nr 94/2025.
[4] Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen, BGBl I Nr 60/2025.
[5] Verordnung des Bundesministers für Inneres zur Durchführung des Resilienz kritischer Einrichtungen-Gesetzes

3. Das RKEG betrifft die Resilienz kritischer Einrichtungen und damit die Fähigkeit, wesentliche Dienste auch bei Störungen aufrechtzuerhalten oder rasch wiederherzustellen.

4. Nicht jede Beschaffung einer betroffenen Einrichtung ist im selben Ausmaß „kritisch“. Maßgeblich ist stets der konkrete Zusammenhang zwischen Leistungsgegenstand, Betriebsfunktion, wesentlichem Dienst, Infrastruktur und möglichem Schadensbild.

5. Vor jeder resilienzrelevanten Beschaffung sollte eine kurze Kritikalitätsprüfung dokumentiert werden.

6. Die Leistungsbeschreibung ist der primäre Ort für sicherheits- und resilienzbezogene Mindestanforderungen an die Leistung (Schwerpunkt!).

7. Eignungskriterien dürfen nur echte Mindestfähigkeiten abbilden, da überzogene Zertifikats- oder Referenzanforderungen den Markt unnötig verengen können.

8. Auswahl- und Zuschlagskriterien sollten nur dort eingesetzt werden, wo qualitative Unterschiede transparent beschrieben, überprüfbar bewertet und vertraglich abgesichert werden können.

9. Der Leistungsvertrag macht die Anforderungen während der Vertragslaufzeit prüfbar, steuerbar und sanktionierbar.

10. Standardbausteine erleichtern den Einstieg. Für Hochrisikoprojekte bleiben sie jedoch bloßer Ausgangspunkt und sind nicht der Endpunkt der Ausarbeitung.

3. Ein Überblick: NISG 2026, RKEG und Vergaberecht

3.1. Zwei Regelungswerke, ein gemeinsamer Beschaffungsbezug

Wer resilienzorientiert beschaffen will, muss zunächst die Grundidee von NISG 2026 und RKEG verstehen. Das NISG 2026 schützt die Cybersicherheit von Netz- und Informationssystemen. Für Beschaffungen wird es vor allem dann relevant, wenn externe Auftragnehmer mit IT-/OT-Systemen, digitalen Betriebsprozessen oder sonstigen Netz- und Informationssystemen in Berührung kommen, die für die Cybersicherheit der Einrichtung wesentlich sind. Das kann etwa der Fall sein, wenn Auftragnehmer Systeme betreiben, warten, administrieren, absichern oder im Störungsfall wiederherstellen sollen. Relevant sind außerdem Beschaffungen, bei denen sicherheitskritische Liefer- oder Dienstleistungsketten eingebunden werden. Dann müssen im Vergabeverfahren die erforderlichen Anforderungen an Leistungsinhalt, Eignung und Nachweise festgelegt werden. Der Leistungsvertrag muss ergänzend sicherstellen, dass Vorfälle gemeldet, Wiederherstellungsleistungen erbracht und die für Aufsicht, Dokumentation und Nachweisführung erforderlichen Informationen bereitgestellt werden.

Das RKEG setzt an einer anderen Stelle an. Es schützt die Fähigkeit kritischer Einrichtungen, wesentliche Dienste auch bei Störungen, Angriffen, Ausfällen oder sonstigen Sicherheitsvorfällen aufrechtzuerhalten oder rasch wiederherzustellen. Für Beschaffungen bedeutet das: Nicht nur technische Systeme, sondern auch Anlagen, Standorte, Personal, Zutritt, Subunternehmer, Notfallprozesse und Wiederanlauf können relevant werden. Die folgende Übersichtslandkarte zeigt, wie beide Regelungswerke funktionieren und wie ihre Anforderungen in der Vergabepraxis richtig eingeordnet werden.

Für die Vergabepraxis ist daher zunächst zwischen zwei Blickrichtungen zu unterscheiden: Das NISG 2026 fragt aus der Perspektive der Cybersicherheit, welche Anforderungen an Netz- und Informationssysteme, digitale Betriebsprozesse und deren externe Unterstützung zu stellen sind. Das RKEG fragt aus der Perspektive der Aufrechterhaltung wesentlicher Dienste, welche organisatorischen, physischen und personellen Abhängigkeiten für die Resilienz kritischer Einrichtungen relevant sind. Beide Perspektiven können denselben Beschaffungsvorgang betreffen, führen aber nicht automatisch zu denselben vergaberechtlichen Anforderungen.

3.2. Was ist das NISG 2026?

Das NISG 2026 ist das österreichische Umsetzungsgesetz zur NIS-2-Richtlinie. Es soll ein hohes Cybersicherheitsniveau von Netz- und Informationssystemen gewährleisten. Der Anwendungsbereich ist deutlich weiter als jener des früheren NISG 2018[6]. Er erfasst wesentliche und wichtige Einrichtungen in zahlreichen Sektoren, darunter **Energie, Verkehr, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, Abfallbewirtschaftung, öffentliche Verwaltung, Verwaltung von IKT-Diensten und weitere Bereiche wie zB Produktion, Verarbeitung und Vertrieb von Lebensmitteln**.

Die Einstufung folgt im Ausgangspunkt einer Kombination aus Sektorzuordnung und Unternehmensgröße. Daneben bestehen auch größenunabhängige Einstufungen, etwa für bestimmte digitale Dienste oder für Einrichtungen, die nach der RKE-Richtlinie beziehungsweise nach dem RKEG als kritische Einrichtungen ermittelt wurden. Für öffentliche Verwaltungseinrichtungen gelten Sonderregeln.

Das NISG 2026 macht organisatorische Cybersicherheit zu einer **verbindlichen Management- und Governance-Aufgabe**. Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige Risikomanagementmaßnahmen setzen, ihre Leitungsorgane einbinden, Schulungen vorsehen, erhebliche Cybersicherheitsvorfälle melden, Registrierungspflichten erfüllen und ihre Maßnahmen dokumentieren. Cybersicherheit ist damit nicht bloß ein Thema der IT-Abteilung, sondern Teil der gesamten Governance der Einrichtung.

Praxishinweis: Cybersicherheit ist Leitungsthema

Die Verantwortung für Risikomanagement, Schulung, Meldeprozesse und Überwachung liegt auf Leitungsebene. CISO, IT-Abteilung und externe Dienstleister können vorbereiten, beraten und umsetzen. Sie ersetzen aber nicht die Verantwortung der Einrichtung, ihre gesetzlichen Pflichten organisatorisch abzusichern. Im Rahmen von Beschaffungsprozessen müssen externe Leistungen daher so beschrieben und vertraglich geregelt werden, dass die Einrichtung ihre eigenen Nachweis-, Melde- und Steuerungspflichten auch tatsächlich erfüllen kann.

Für die Beschaffung sind vor allem jene NISG-Pflichten relevant, die ohne Mitwirkung externer Leistungsträger praktisch nicht zuverlässig erfüllt werden können. Dazu gehören insbesondere Sicherheitsanforderungen an IT-/OT-Systeme, Lieferkettensteuerung, Incident Management, Notfall- und Krisenmanagement, Backup und Wiederherstellung, Schwachstellenmanagement, sichere Authentifizierungs- und Kommunikationsverfahren, Schulung, Dokumentation und Wirksamkeitsnachweis.

Ein zentraler Risikobereich liegt dabei in der Lieferkette. Auftragnehmer, Hersteller, Wartungsunternehmen, Cloud-Anbieter, Rechenzentrumsbetreiber, Managed-Service-Provider und Subunternehmer können zugleich Leistungserbringer, Schwachstelle, Frühwarnstelle und Wiederherstellungsressource sein. Werden Leistungen beschafft, die für Netz- und Informationssysteme, betriebliche Kernprozesse, Vorfallbewältigung oder Wiederanlauf relevant sind, müssen die erforderlichen Sicherheitsanforderungen zumindest auf der Ebene der Leistungsbeschreibung, der Eignung und des Leistungsvertrags abgebildet werden.

Die Beschaffungsrelevanz des NISG 2026 liegt damit vor allem in der Übersetzung von Cybersicherheits- und Lieferkettenpflichten in konkrete Anforderungen an externe Leistungsträger. Diese Perspektive ist allerdings nur ein Teil des Gesamtbildes. Für kritische Einrichtungen stellt sich zusätzlich die Frage, ob eine Leistung nicht nur digital, sondern auch funktional, physisch und/oder organisatorisch für die Aufrechterhaltung eines wesentlichen Dienstes relevant ist. Damit rückt das RKEG in den Fokus.

3.3. Was ist das RKEG?

Das RKEG setzt die RKE-Richtlinie in Österreich um. Es zielt auf die Widerstandsfähigkeit jener Einrichtungen ab, deren Dienste für zentrale gesellschaftliche, wirtschaftliche oder staatliche Funktionen wesentlich sind. Während

[6] Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, BGBl I Nr 111/2018.

das NISG 2026 vor allem die Cybersicherheit von Netz- und Informationssystemen erfasst, richtet das RKEG den Blick auf die physische, organisatorische und funktionale Widerstandsfähigkeit kritischer Einrichtungen.

Im Mittelpunkt des RKEG stehen nicht sämtliche Unternehmen oder öffentlichen Stellen in sensiblen Bereichen. Erfasst werden öffentliche und private Einrichtungen, die aufgrund ihrer konkreten Funktion, der Bedeutung ihrer Dienste und der dafür erforderlichen Infrastruktur vom Bundesminister für Inneres nach § 11 RKEG mit **Bescheid** als kritische Einrichtungen eingestuft werden. Die Einstufung knüpft insbesondere daran an, dass die Einrichtung in einem erfassten Sektor tätig ist, sich ihre kritische Infrastruktur im Inland befindet, sie einen wesentlichen Dienst erbringt und bei dessen Erbringung ein Sicherheitsvorfall eintreten kann.

Für das Verständnis des RKEG sind drei Begriffe maßgeblich: Der „wesentliche Dienst" ist jene Dienstleistung, deren Aufrechterhaltung für zentrale gesellschaftliche oder wirtschaftliche Funktionen erforderlich ist. Die „kritische Infrastruktur" bezeichnet jene Objekte, Anlagen, Ausrüstungen, Netze, Systeme oder Teile davon, die für die Erbringung dieses Dienstes erforderlich sind. Ein „Sicherheitsvorfall" ist schließlich ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte.

Zudem ist zu berücksichtigen, dass RKEG-relevante Anforderungen an Vergaben nicht nur aus dem Gesetzestext an sich, sondern auch aus den jeweils einschlägigen sektoralen Schwellenwerten und Konkretisierungen gemäß RKEV abzuleiten sind.

Kritische Einrichtungen haben demnach eine Risikoanalyse durchzuführen, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zu setzen und diese in einem Resilienzplan darzustellen. Die Maßnahmen beziehen sich auf den von der kritischen Einrichtung erbrachten wesentlichen Dienst. Genau hier entsteht die Brücke zur Beschaffung: Werden externe Leistungen für Betrieb, Absicherung, Aufrechterhaltung und/oder Wiederherstellung eines wesentlichen Dienstes benötigt, müssen die entsprechenden Anforderungen gegenüber Auftragnehmern abgebildet und durchsetzbar gemacht werden.

Merke:
RKEG-Resilienz ist mehr als Objektschutz. Sie betrifft die Fähigkeit einer kritischen Einrichtung, wesentliche Dienste auch bei Störungen aufrechtzuerhalten oder rasch wiederherzustellen. Beschaffungsrelevant werden daher vor allem externe Abhängigkeiten, Personal, Subunternehmer, Vorfallkommunikation, Wiederanlaufprozesse und vertragliche Durchgriffsrechte.

Die Resilienz kritischer Einrichtungen hängt nicht nur von Anlagen, Systemen und Prozessen ab. Gerade in der Beschaffung stellt sich auch die Frage, welche Personen später tatsächlich Zutritt zu sensiblen Bereichen erhalten, auf Systeme zugreifen können oder in Störungs- und Notfallsituationen handeln müssen. Die Sicherstellung der Zuverlässigkeit des eingesetzten Personals ist daher ein eigenständiges und praktisch besonders wichtiges Beschaffungsthema.

Das RKEG enthält eigene Regelungen zu Zuverlässigkeitsüberprüfungen des eingesetzten Personals. Diese betreffen sensible personenbezogene Daten, Strafregisterbescheinigungen beziehungsweise vergleichbare Nachweise sowie Kriterien wie einschlägige Verurteilungen, anhängige Verfahren, Waffenverbote oder Naheverhältnisse zu extremistischen, terroristischen und/oder kriminellen Gruppierungen. Für Vergabeverfahren folgt daraus aber kein Freibrief, pauschal „Background Checks" oder Strafregisterauszüge für sämtliche Mitarbeitenden von Auftragnehmern zu verlangen. Es gilt – auch in diesem Fall – das vergaberechtliche Verhältnismäßigkeitsprinzip.

3.4. Wie hängen NISG 2026 und RKEG zusammen?

Für die Vergabepraxis entscheidend ist weniger die isolierte Betrachtung von NISG 2026 und RKEG, sondern ihr funktionales Zusammenwirken. Viele Beschaffungen berühren zugleich digitale Systeme, physische Infrastruktur, betriebliche Abhängigkeiten und Wiederanlaufprozesse. Gerade dort sind NISG 2026 und RKEG gemeinsam zu berücksichtigen, ohne sie miteinander zu vermengen.

NISG 2026 und RKEG verfolgen – wie bereits aufgezeigt – nämlich unterschiedliche Schutzrichtungen. Das NISG 2026 adressiert Cybersicherheit, Netz- und Informationssysteme, IT- und OT-Risiken, digitale Sicherheitsvorfälle,

Lieferkettensicherheit und Cybersicherheits-Governance. Das RKEG adressiert die Resilienz kritischer Einrichtungen, wesentliche Dienste, kritische Infrastruktur, physische und organisatorische Widerstandsfähigkeit, Resilienzpläne und Sicherheitsvorfälle unabhängig von ihrer Ursache.

In der Praxis überschneiden sich beide Regelungswerke dort, wo digitale Systeme für physische oder organisatorische Resilienz erforderlich sind. Beispiele sind Prozessleitsysteme, Fernwirksysteme, Rechenzentren, Cloud-Dienste, Kommunikationsnetze, Zutritts- und Berechtigungssysteme, Ersatzteillogistik, Notfallkommunikation und Wiederanlaufplanung.

Frage	NISG 2026	RKEG
Fokus	Cybersicherheit von Netz- und Informationssystemen	Physische, organisatorische und funktionale Resilienz kritischer Einrichtungen
Betroffene	wesentliche und wichtige Einrichtungen (§ 2)	durch Bescheid ermittelte kritische Einrichtungen (§ 11)
Schutzgegenstand	Netz- und Informations-systeme samt relevanter Prozesse	wesentliche Dienste und dafür erforderliche kritische Infrastruktur
Typische Beschaffungsthemen	IT/OT, Cloud, Managed Services, Incident Handling, Schwachstellenmanagement, Lieferkette	Anlagen, Standorte, Zutritt, Personal, Wiederanlauf, Notfallprozesse, externe Abhängigkeiten
Vertragsrelevanz	Meldung, Nachweis, Sicherheitsmaßnahmen, Lieferkette, Auditierbarkeit	Resilienzmaßnahmen, Personal, Zutritt, Vorfallkommunikation, Wiederherstellung, Durchgriff auf Dritte

Beide Regelungswerke dürfen nicht schematisch addiert werden. Nicht jede NISG-relevante IT-Leistung ist automatisch eine RKEG-Leistung und nicht jede RKEG-relevante Beschaffung ist automatisch ein Cyber-Hochrisikoprojekt. Entscheidend bleibt der konkrete Beschaffungsgegenstand und seine Bedeutung für Netz- und Informationssysteme, wesentliche Dienste, kritische Infrastruktur, Betriebsprozesse, Lieferketten, Vorfallbewältigung und Wiederanlauf.

Merke:
NISG 2026 und RKEG sind zwei „Sicherheitsraster“ mit unterschiedlicher Zielrichtung. In resilienzrelevanten Beschaffungen müssen sie daher übereinandergelegt werden, ohne dass dabei ihre Unterschiede vermengt werden.

Die entscheidende praktische Frage lautet daher nicht, welches Gesetz abstrakt „wichtiger“ ist. Entscheidend ist, welche Anforderungen sich aus beiden Regelungswerken für die **jeweils konkrete Beschaffung** ableiten lassen.

4. Warum der Einkauf Resilienzanforderungen berücksichtigen muss

Beschaffung ist der strategische Knotenpunkt, in dem Sicherheits- und Resilienzanforderungen rechtssicher, wettbewerblich geordnet und vertraglich durchsetzbar festgelegt werden können. Was in der Ausschreibung und im Vertrag nicht geregelt ist, lässt sich nach Zuschlag gar nicht oder nur eingeschränkt (und häufig mit Mehrkosten, Änderungsrisiken oder vergaberechtlichen Folgefragen behaftet) nachschärfen.

Das gilt besonders für Leistungen, die kritische Infrastruktur, betriebsnahe IT-/OT-Systeme, Wartung, Bereitschaft, Support, Zutritt, Subunternehmer, Ersatzteile, Notfallprozesse oder Wiederanlauf berühren. Externe Auftragnehmer sind in solchen Fällen mehr als bloße Erfüllungsgehilfen: Sie können auch Risikoquelle, Kontrollpunkt, Frühwarnstelle, Nachweisträger und Wiederherstellungsressource sein.

Die Vergabeunterlagen sollten in diesem Zusammenhang jedoch nicht mit möglichst vielen Kriterien überladen werden. Erforderlich ist eine saubere Zuordnung der Themen zu den richtigen Vergabehebeln: Die **„Leistungsbeschreibung“** legt fest, was die Leistung können muss. Die **„Eignung“** prüft, ob der Bieter die Mindestfähigkeit zur Leistungserbringung besitzt. **„Auswahlkriterien“** identifizieren in bestimmten Verfahren ein Mehr an unternehmerischer Qualität. **„Zuschlagskriterien“** berücksichtigen echte leistungsbezogene Mehrwerte. Der **„Leistungsvertrag“** macht die Anforderungen während der Laufzeit operationalisierbar und durchsetzbar.

5. Am Anfang steht die Kritikalitätsprüfung

5.1. Zweck der Kritikalitätsprüfung

Vor Einleitung eines Vergabeverfahrens sollte der Auftraggeber prüfen, ob die ausgeschriebene Leistung ein **„Standardprojekt“**, ein **„Risikoprojekt“** oder ein **„Hochrisikoprojekt“** ist. Diese Einstufung entscheidet darüber, welche Anforderungen erforderlich, verhältnismäßig und somit marktschonend sind.

Ein „Standardprojekt“ liegt vor, wenn ein Ausfall oder eine mangelhafte Leistungserbringung keine oder nur unwesentliche Auswirkungen auf Versorgungssicherheit, wesentliche Dienste, kritische Infrastruktur, IT-/OT-Systeme, Betriebsprozesse, Sicherheitsvorfälle oder Wiederanlaufprozesse hätte.

Ein „Risikoprojekt“ liegt vor, wenn die Leistung sicherheits- oder resilienzrelevante Schnittstellen aufweist, ohne bereits die Komplexität eines Hochrisikoprojekts zu erreichen.

Ein „Hochrisikoprojekt“ liegt vor, wenn Ausfall, Kompromittierung oder Fehlleistung erhebliche Auswirkungen auf wesentliche Dienste, kritische Infrastruktur, Versorgungssicherheit, zentrale IT-/OT-Systeme oder Wiederanlauffähigkeit haben können.

5.2. Muster: Einfache Kritikalitätsprüfung

Es empfiehlt sich somit, noch vor Einleitung des Vergabeverfahrens im Vergabeakt kurz zu dokumentieren, ob und in welchem Ausmaß die ausgeschriebene Leistung sicherheits- und/oder resilienzrelevante Funktionen betrifft. Dabei sind insbesondere folgende Prüffragen geeignet:

- Ist die Leistung für die Erbringung eines wesentlichen Dienstes relevant?
- Betrifft die Leistung kritische Infrastruktur und/oder deren Betrieb, Wartung, Schutz und/oder Wiederherstellung?
- Erfordert die Leistung Zugang zu Betriebsstätten, Baustellen, Anlagen, Leitstellen, Rechenzentren, IT-/OT-Systemen oder sonstigen sicherheitsrelevanten Bereichen?
- Kann die Leistung Verfügbarkeit, Integrität, Vertraulichkeit oder Wiederherstellbarkeit von Daten, Systemen oder Betriebsprozessen beeinflussen?

- Ist die Leistung für Vorfallmanagement, Notbetrieb, Wiederanlauf oder Business Continuity relevant?
- Werden Subunternehmer, Lieferketten oder externe Dienstleister mit sicherheitsrelevanter Wirkung eingebunden?
- Kann ein Ausfall erhebliche Auswirkungen auf Versorgungssicherheit, öffentliche Sicherheit, Gesundheit, Umwelt, wirtschaftliche Tätigkeit oder Betriebskontinuität haben?

Das Ergebnis ist knapp, aber nachvollziehbar im Vergabeakt festzuhalten. Aus der Einstufung muss erkennbar sein, weshalb bestimmte Anforderungen vorgesehen, abgeschwächt oder bewusst nicht aufgenommen wurden. Eine entsprechende Dokumentation ist insbesondere auch im Hinblick auf die Business-Judgement-Rule empfehlenswert bzw entspricht der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsmannes (vgl § 25 Abs 1 und Abs 1a GmbH-Gesetz).

5.3. Muster: Kurze Risikomatrix

Auswirkung bei Ausfall/ Kompromittierung	**Eintritts-wahrscheinlichkeit** **niedrig**	**Eintritts-wahrscheinlichkeit** **mittel**	**Eintritts-wahrscheinlichkeit** **hoch**
gering	Standardprojekt	Standardprojekt	Risikoprojekt
erheblich	Risikoprojekt	Risikoprojekt	Hochrisikoprojekt
kritisch	Hochrisikoprojekt	Hochrisikoprojekt	Hochrisikoprojekt

Als „geringe Auswirkung“ gelten Folgen, die ohne wesentliche Beeinträchtigung betrieblicher oder sicherheitsrelevanter Funktionen kompensiert werden können. „Erhebliche Auswirkungen“ betreffen betriebliche Kernprozesse, sicherheitsrelevante Schnittstellen, einzelne Anlagen, unterstützende IT-Systeme, Lieferketten oder Wiederanlaufprozesse. „Kritische Auswirkungen“ liegen vor, wenn wesentliche Dienste, kritische Infrastruktur, zentrale IT-/OT-Systeme, Versorgungssicherheit, Gesundheit oder Sicherheit der Bevölkerung oder die Fähigkeit zur Vorfallbewältigung betroffen sein können.

Merke:
Die Risikomatrix ist eine grobe Verortung für die Praxis und soll öffentliche Auftraggeber zu einer bewussten, dokumentierten Entscheidung anleiten, welche Beschaffungskategorie vorliegt und weshalb bestimmte Anforderungen vorgesehen oder bewusst nicht vorgesehen werden.

6. Basistoolbox für Risikoprojekte

Risikoprojekte verlangen nicht in jedem Fall ISO-Zertifizierungen, externe Prüfberichte oder komplexe Zuschlagsmodelle. Gerade für kleinere Beschaffungsvorhaben werden Bausteine benötigt, die rechtlich tragfähig, praktisch handhabbar und für den Markt zumutbar sind. Das **vergaberechtliche Verhältnismäßigkeitsprinzip und Sachlichkeitsgebot** sind stets zu berücksichtigen. Folgende Basistools können herangezogen werden:

Basistools	Zweck
Kritikalitätsprüfung	Dokumentiert, warum ein Projekt als Standardprojekt, Risikoprojekt oder Hochrisikoprojekt qualifiziert wird.
Risikomatrix	Schafft eine einfache, nachvollziehbare Einstufung nach Auswirkung und Eintrittswahrscheinlichkeit.
Vertraulichkeitsklausel	Schützt Informationen über Anlagen, Systeme, Betriebsprozesse, Schwachstellen und Notfallkonzepte.
Incident-Meldeklausel	Sichert rasche und strukturierte Information bei sicherheits- oder betriebsrelevanten Ereignissen.
Subunternehmer-Genehmigungsvorbehalt	Verhindert unkontrollierte Weitergabe sensibler Leistungsteile.
Zutritts- und Ausweisregelung	Stellt sicher, dass nur bekannte und berechtigte Personen sensible Bereiche betreten.
Sicherheitsunterweisung	Sorgt dafür, dass eingesetztes Personal die relevanten Sicherheits- und Meldepflichten kennt.
Personalzuverlässigkeit	Regelt, dass nur geeignetes, geschultes und zuverlässiges Personal eingesetzt wird.

Praxishinweis: Nicht jedes Risiko rechtfertigt Maximalanforderungen

Resilienzorientierte Beschaffung bedeutet nicht, jedes Projekt mit Zertifikaten, umfangreichen Konzepten, Background Checks und Auditregimen auszustatten. Anforderungen müssen mit dem Auftragsgegenstand verbunden (Sachlichkeitsgebot) und marktschonend sein (Verhältnismäßigkeitsprinzip). In regionalen Märkten können Eigenerklärungen, Referenzen, klare Mindestpflichten und einfache Vertragsbausteine zweckmäßiger sein als formale Zertifikatsanforderungen.

7. Vergabeinstrumente im Überblick

7.1. Vom Risiko zur Ausschreibung: Wo Anforderungen richtig geregelt werden

Nachdem die Kritikalität der Beschaffung bestimmt wurde, stellt sich die zentrale vergaberechtliche Folgefrage: Wo werden die jeweiligen Sicherheits- und Resilienzanforderungen richtig verankert? Nicht jede Anforderung gehört an dieselbe Stelle der Ausschreibung. Manche Vorgaben beschreiben unmittelbar die geschuldete Leistung, andere betreffen die Mindestfähigkeit des Bieters, wieder andere eignen sich nur als bewertbarer qualitativer Mehrwert oder müssen im Leistungsvertrag für die Vertragslaufzeit operationalisiert werden.

Die richtige Zuordnung ist für die Rechtssicherheit und Praxistauglichkeit des Vergabeverfahrens entscheidend. Wird eine Anforderung an der falschen Stelle geregelt, kann sie entweder vergaberechtlich angreifbar, praktisch schwer überprüfbar oder später vertraglich nur eingeschränkt durchsetzbar sein. Der Auftraggeber sollte daher bereits bei der Erstellung der Vergabeunterlagen festlegen, ob ein bestimmtes Thema in die Leistungsbeschreibung, in die Eignung, in die Auswahl, in den Zuschlag oder in den Leistungsvertrag gehört.

Die nachstehenden Vergabeinstrumente werden daher der Reihe nach dargestellt. Sie bilden jene Stellen im Vergabeverfahren, an denen resilienzbezogene Anforderungen niedergeschrieben, konkretisiert, bewertet oder für die spätere Vertragsdurchführung verbindlich gemacht werden können. Die Grundlogik ist folgende: Die Leistungsbeschreibung definiert, was die Leistung können muss (Schwerpunkt); die Eignung stellt sicher, dass nur geeignete Unternehmen zugelassen werden; Auswahl- und Zuschlagskriterien dürfen nur echte und überprüfbare Qualitätsunterschiede erfassen und der Leistungsvertrag macht die Anforderungen während der Vertragslaufzeit steuerbar und durchsetzbar.

7.2. Leistungsbeschreibung

Die Leistungsbeschreibung ist der primäre Ort der Resilienzsteuerung, weil sie den geschuldeten Leistungsinhalt festlegt. Sie beantwortet die Frage, was die Leistung können muss: welches Sicherheitsniveau einzuhalten ist, welche Verfügbarkeit erwartet wird, welche Schnittstellen geschützt werden müssen, welche Dokumentation zu liefern ist und welche Mindestanforderungen an Vorfallmeldung, Wiederanlauf, Personal, Subunternehmer und Nachvollziehbarkeit gestellt werden.

Der Leistungsvertrag beantwortet demgegenüber die Frage, wie diese Anforderungen während der Vertragslaufzeit umgesetzt, kontrolliert und durchgesetzt werden. Er regelt Meldefristen, Nachweise, Auditrechte, Eskalation, Sanktionen, Kündigungsrechte, Änderungsmechanismen, Mitwirkungspflichten und Exit. Leistungsbeschreibung und Vertrag ergänzen sich somit. Die Leistungsbeschreibung definiert das Soll; der Vertrag macht dieses Soll steuerbar.

Thema	In die Leistungsbeschreibung gehört	In den Leistungsvertrag gehört
Sicherheitsniveau	Mindestanforderungen an Schutzbedarf, Stand der Technik, technische und organisatorische Maßnahmen	laufende Aufrechterhaltung, Aktualisierung, Nachweisführung, Rechtsfolgen bei Abweichungen
Verfügbarkeit	geforderte Servicezeiten, Mindestverfügbarkeit, Reaktions- und Wiederherstellungsziele	SLA-Regime, Reporting, Pönalen, Eskalation, Kündigungsrechte
Incident Management	Mindestanforderung an Meldeprozess, Meldekategorien und Ansprechbarkeit	konkrete Meldefristen, Mindestinhalte, Eskalationswege, Mitwirkung, Sanktionen
Wiederanlauf	Anforderungen an Notbetrieb, Backup, Wiederherstellung, RTO/RPO	Testpflichten, Übungsrechte, Nachweispflichten, Unterstützung im Ernstfall
Personal	Mindestqualifikation, Schlüsselrollen, Schulungserfordernisse	Unterweisung, Einsatzlisten, Austausch, Ablehnungsrechte, Zutrittsregeln
Subunternehmer	sensible Leistungsteile, Zulässigkeit oder Beschränkung von Subunternehmern	Genehmigungsvorbehalt, Weitergabepflichten, Haftung, Auditierbarkeit
Dokumentation	Art und Umfang der zu liefernden Dokumente	Aktualisierung, Herausgabe, Aufbewahrung, Einsichtsrechte
Logging	Mindestanforderungen an Nachvollziehbarkeit sicherheitsrelevanter Vorgänge	Aufbewahrungsdauer, Anlasszugriff, Datenschutz, Manipulationsschutz
Behördenmitwirkung	Anforderung, dass Unterstützung bei gesetzlichen Pflichten möglich sein muss	Fristen, Form, Ansprechpartner, Kostenregelung, Haftung

Exit	funktionale Übergabefähigkeit, Portabilität, Dokumentationsstand	Exitplan, Übergabefristen, Rückgabe/Löschung, Unterstützung eines Nachfolgeauftragnehmers

Jedes Beschaffungsvorhaben hat eigene technische, organisatorische und rechtliche Besonderheiten. Die sicherheits- und resilienzbezogenen Grundanforderungen folgen jedoch häufig einer ähnlichen Logik: Die Leistung muss sicher erbracht werden, Störungen müssen rasch erkannt und gemeldet werden, eingesetztes Personal muss geschult und zuverlässig sein, Subunternehmer müssen kontrolliert werden, sicherheitsrelevante Tätigkeiten müssen nachvollziehbar bleiben und der Auftraggeber muss im Anlassfall die für seine eigenen Nachweis-, Auskunfts- und Meldepflichten erforderlichen Informationen erhalten.

Das folgende Muster versteht sich daher als generalisierte Basisvorgabe für Risikoprojekte. Es ersetzt keine projektspezifische Leistungsbeschreibung, schafft aber ein belastbares Grundgerüst, das in vielen Beschaffungsvorhaben als Ausgangspunkt verwendet und je nach Kritikalität, Leistungsgegenstand und Marktumfeld ergänzt, präzisiert oder reduziert werden kann.

Muster: Sicherheits- und Resilienzanforderungen in der Leistungsbeschreibung

Der Auftragnehmer hat die Leistung so zu erbringen, dass die Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und Nachvollziehbarkeit der vom Auftrag betroffenen Systeme, Anlagen, Informationen und Betriebsprozesse angemessen gewahrt bleiben. Der Auftragnehmer hat insbesondere

a. die für die Leistungserbringung relevanten Sicherheits- und Zutrittsvorgaben des Auftraggebers einzuhalten,

b. sicherheits- oder betriebsrelevante Störungen unverzüglich an den Auftraggeber zu melden,

c. eingesetztes Personal vor Leistungsbeginn über die relevanten Sicherheits-, Vertraulichkeits-, Zutritts- und Meldepflichten zu unterweisen,

d. Subunternehmer nur nach Maßgabe der Ausschreibungs- und Vertragsbestimmungen einzusetzen,

e. sicherheitsrelevante Tätigkeiten nachvollziehbar zu dokumentieren,

f. an der Analyse, Eindämmung und Behebung von Sicherheits- oder Betriebsstörungen mitzuwirken,

g. vertrauliche Informationen des Auftraggebers zu schützen und

h. den Auftraggeber bei der Erfüllung gesetzlicher Auskunfts-, Nachweis- und Meldepflichten angemessen zu unterstützen, soweit diese mit der vertragsgegenständlichen Leistung zusammenhängen.

7.3. Eignungskriterien

Die Leistungsbeschreibung legt fest, welche Anforderungen die ausgeschriebene Leistung erfüllen muss. Daran schließt die Eignungsprüfung an: Sie betrifft nicht mehr das „Was“ der Leistung, sondern das „Wer“ der Leistungserbringung. Es ist zu prüfen, welche Mindestfähigkeiten ein Unternehmen besitzen muss, um die beschriebene Leistung sicher, verlässlich und im Einklang mit den resilienzbezogenen Anforderungen erbringen zu können.

Eignungskriterien dienen dazu, nur solche Unternehmen zum Verfahren zuzulassen, die über die erforderliche Befugnis, Zuverlässigkeit und Leistungsfähigkeit verfügen. Sie wirken als Marktzugangsschwelle und sind daher besonders sorgfältig zu wählen. Zu niedrige Anforderungen können dazu führen, dass Auftragnehmer zugelassen werden, die sicherheits- oder resilienzrelevante Leistungen nicht ausreichend beherrschen. Zu hohe Anforderungen können den Wettbewerb unnötig verengen und geeignete Anbieter ausschließen.

Bei Risikoprojekten kommen insbesondere einschlägige Referenzen, Erfahrung in sicherheits- oder betriebsrelevanten Umgebungen, geeignete Organisationsstrukturen, qualifiziertes Schlüsselpersonal, ausreichender Versicherungsschutz, eine nachvollziehbare Subunternehmerstruktur und organisatorische Mindestprozesse für Störungen, Sicherheitsvorfälle und Eskalationen in Betracht. Zertifizierungen wie ISO/IEC 27001 oder ISO 22301

können sinnvoll sein, sollten aber nicht reflexartig verlangt werden. In vielen Märkten gibt es geeignete Anbieter, die kein bestimmtes Zertifikat besitzen, aber gleichwertige Organisation, einschlägige Erfahrung und belastbare Nachweise vorlegen können.

KMU-freundliche Vergabe: Insbesondere kleinere Auftraggeber (zB Gemeinden, kleine Körperschaften öffentlichen Rechts) und kleinere Beschaffungsvorhaben erfordern eine verhältnismäßige Anpassung der Anforderungen. Strenge Zertifizierungspflichten (zB ISO 27001, ISO 22301) können den Bietermarkt erheblich einschränken und faktisch auf wenige Großanbieter reduzieren, was dem vergaberechtlichen Wettbewerbsgrundsatz widerspricht. Kleinere Auftraggeber sollten daher – abhängig vom Risikoprofil des Vorhabens – auf ein abgestuftes Anforderungsniveau setzen, das Sicherheitsaspekte angemessen berücksichtigt, ohne den Wettbewerb unverhältnismäßig einzuschränken. Darüber hinaus ist darauf hinzuweisen, dass bei Zertifizierungsvorgaben im Bereich der Eignung nur auf Qualitätssicherungssysteme Bezug genommen werden darf, die den einschlägigen europäischen Normen genügen und von akkreditierten Stellen zertifiziert sind (§ 87 BVergG 2018).

Vor diesem Hintergrund empfiehlt es sich zuweilen, nur einzelne – den jeweiligen Zertifizierungen zugrunde liegende und für das jeweilige Projekt relevante – Anforderungen als Eignungskriterien heranzuziehen (und nicht die Zertifizierung selbst) und die konkrete Nachweisführung für die entsprechende Anforderung dem Bieter offen zu lassen.

Die Eignung ist damit kein Instrument zur Bewertung des besten Angebots, sondern zur Festlegung der unternehmerischen Mindestfähigkeit. Was ein Unternehmen mindestens können muss, gehört in die Eignung. Was die angebotene Leistung besser macht, gehört – sofern objektiv bewertbar – in den Zuschlag oder als Mindestanforderung in die Leistungsbeschreibung.

Praxishinweis: Zertifikate sind Nachweise, keine Ersatz-Compliance

Zertifizierungen können ein starkes Indiz für strukturierte Informationssicherheit oder Business Continuity sein. Sie ersetzen aber nicht die Prüfung, ob die konkreten Anforderungen des NISG 2026, des RKEG, der Leistungsbeschreibung und des Vertrages erfüllt werden. Auftraggeber müssen Zertifikate jedenfalls gleichwertigkeitsoffen und verhältnismäßig einsetzen. Eine Zertifizierung darf somit nicht als Ersatz für konkrete Leistungs-, Melde-, Mitwirkungs- und Nachweispflichten verstanden werden, sondern als ein möglicher Nachweis innerhalb eines insgesamt stimmigen Sicherheits- und Resilienzkonzepts.

Neben der unternehmensbezogenen Eignung des Bieters stellt die Zuverlässigkeit des tatsächlich eingesetzten Personals – insbesondere bei sicherheitsrelevanten Vorhaben im Anwendungsbereich des NISG 2026 und des RKEG – eine eigenständige und häufig unterschätzte Anforderung dar. Sicherheitsvorfälle gehen in der Praxis nicht selten auf menschliches Versagen, Unachtsamkeit oder – im Extremfall – auf böswilliges Handeln von Mitarbeitenden des Auftragnehmers zurück. Auftraggeber müssen daher abwägen, ob sie nicht nur das Unternehmen als solches, sondern auch das konkret eingesetzte Personal einer angemessenen Überprüfung unterziehen müssen. Als Nachweise kommen insbesondere Eigenerklärungen des Auftragnehmers, Lebensläufe und Qualifikationsnachweise benannter Schlüsselpersonen sowie die Darstellung eines internen Personalauswahlverfahrens in Betracht, das Zuverlässigkeitsaspekte berücksichtigt. Bei Hochrisikoprojekten können darüber hinaus weitergehende Nachweise erforderlich sein, etwa Strafregisterbescheinigungen oder Zuverlässigkeitsüberprüfungen.

Muster: Vertragliche Klausel „Zuverlässigkeit des eingesetzten Personals“

Der Auftragnehmer verpflichtet sich, ausschließlich solches Personal auf dem gegenständlichen Auftrag einzusetzen, das

a. *fachlich für die übertragenen Aufgaben qualifiziert ist,*

b. *keine rechtskräftigen Verurteilungen wegen Straftaten aufweist, die Zweifel an der Vertrauenswürdigkeit im gegenständlichen Auftragskontext begründen (insbesondere im Bereich Computerkriminalität, Datenmissbrauch, Betrug oder Sabotage),*

c. *vor Einsatzbeginn über die geltenden Sicherheits- und Vertraulichkeitspflichten informiert und entsprechend belehrt wurde sowie*

d. *eine Vertraulichkeitserklärung unterzeichnet hat.*

Der Auftragnehmer hat auf Verlangen des Auftraggebers nachzuweisen, dass diese Anforderungen für konkret eingesetzte Personen erfüllt sind.

Der Auftraggeber ist berechtigt, vor Beginn der Leistungserbringung eine Liste der vorgesehenen Personen zu verlangen, Änderungen rechtzeitig bekanntzugeben und den Einsatz einzelner Personen aus sachlichen Gründen (zB Sicherheitsüberlegungen) abzulehnen oder deren Austausch zu verlangen. In diesem Fall hat der Auftragnehmer unverzüglich eine qualifizierte Ersatzperson zu stellen.

Der Verstoß gegen diese Pflichten ist mit einer verschuldensabhängigen Vertragsstrafe in Höhe von EUR [XXX] je Einzelfall pönalisiert und stellt einen Grund zur außerordentlichen Kündigung dar.

Muster: Eignungskriterium Referenz

Der Bieter hat seine technische und organisatorische Leistungsfähigkeit durch mindestens ein geeignetes Referenzprojekt aus den letzten <<Jahre>> Jahren nachzuweisen. Die Referenz muss mit der ausgeschriebenen Leistung nach Art, Umfang, Komplexität und sicherheits- beziehungsweise betriebsrelevanter Einbindung vergleichbar sein.

Die Referenz hat zumindest folgende Angaben zu enthalten:

a) *Auftraggeber der Referenzleistung,*

b) *Leistungszeitraum,*

c) *Leistungsgegenstand,*

d) *betroffene Anlagen, Systeme, Betriebsbereiche oder Schnittstellen, soweit deren Offenlegung zulässig ist,*

e) *Darstellung der vom Bieter wahrgenommenen Sicherheits-, Zutritts-, Störungs-, Dokumentations- und/oder Mitwirkungspflichten,*

f) *Bestätigung der ordnungsgemäßen Leistungserbringung durch den Referenzauftraggeber oder gleichwertiger Nachweis.*

Sofern die Referenz sicherheitsrelevante Informationen enthält, kann der Bieter diese in anonymisierter oder abstrahierter Form darstellen, sofern die Vergleichbarkeit der Referenz für den Auftraggeber überprüfbar bleibt.

Muster: Organisation für Sicherheits- und Störungsmanagement

Der Bieter hat nachzuweisen, dass er über eine für die ausgeschriebene Leistung geeignete Organisation zur Behandlung von Störungen, Sicherheitsvorfällen und Eskalationen verfügt. Der Nachweis kann insbesondere durch eine kurze Beschreibung der internen Zuständigkeiten, Eskalationswege, Erreichbarkeiten, Vertretungsregelungen, Dokumentationsprozesse und Subunternehmersteuerung erbracht werden.

Ein zertifiziertes Managementsystem ist für dieses Eignungskriterium nicht zwingend erforderlich. Gleichwertige organisatorische Nachweise sind zulässig, sofern sie die für die konkrete Leistung erforderliche Wirksamkeit nachvollziehbar belegen.

Muster: Zertifiziertes Informationssicherheitsmanagementsystem

Der Bieter hat nachzuweisen, dass er über ein wirksames Informationssicherheitsmanagementsystem verfügt, das für den Leistungsgegenstand geeignet ist. Der Nachweis kann durch ein gültiges Zertifikat nach ISO/IEC 27001 oder durch einen gleichwertigen Nachweis erbracht werden.

Als gleichwertig gelten Nachweise, aus denen sich nachvollziehbar ergibt, dass der Bieter über strukturierte Prozesse zur Risikoanalyse, Zugriffskontrolle, Incident-Behandlung, Wirksamkeitsprüfung, Dokumentation, Lieferkettensteuerung und kontinuierlichen Verbesserung verfügt. Der Auftraggeber behält sich vor, die Gleichwertigkeit anhand der vorgelegten Unterlagen zu prüfen.

7.4. Auswahlkriterien

Nicht jedes Verfahren benötigt Auswahlkriterien, sondern nur zweistufige Vergabeverfahren (zB das Verhandlungsverfahren mit vorheriger Bekanntmachung). Wo sie eingesetzt werden, dienen sie nicht der Bewertung des Angebots, sondern der Auswahl jener Bewerber, die zur Angebotslegung eingeladen werden. Sie stehen daher zwischen Eignung und Zuschlag: Mehr als Mindestfähigkeit, aber noch keine Angebotsqualität. Inhaltlich sind sie ein Mehr an Eignung. Bei Risikoprojekten kommen zusätzliche einschlägige Referenzen, besondere Erfahrung des Schlüsselpersonals oder besondere Erfahrung mit sicherheitsrelevanten Betriebsumgebungen in Betracht.

Auswahlkriterien bewerten ausschließlich die Qualität des Unternehmens, nicht (!) hingegen die konkrete Qualität des Angebots. Die Qualität des Angebots gehört in die Leistungsbeschreibung oder – bei objektiver Bewertbarkeit – in den Zuschlag.

Muster: Zusätzliche Referenzen

Geeignete Bewerber erhalten zusätzliche Punkte, wenn sie über die Mindestanforderungen hinaus weitere einschlägige Referenzen nachweisen. Gewertet werden maximal <<Anzahl>> zusätzliche Referenzen, die mit der ausgeschriebenen Leistung nach Art, Umfang, Komplexität und sicherheits- beziehungsweise betriebsrelevanter Einbindung vergleichbar sind.

Die Bewertung erfolgt wie folgt:

a) <<Anzahl>> Punkte für jede zusätzliche vergleichbare Referenz,

b) zusätzlich <<Anzahl>> Punkte, wenn die Referenz Leistungen in einer kritischen oder besonders betriebsrelevanten Umgebung betrifft,

c) zusätzlich <<Anzahl>> Punkte, wenn die Referenz dokumentierte Störungs-, Incident-, Wiederanlauf- und/oder Subunternehmersteuerung umfasst.

Die maximale Punktezahl beträgt <<Anzahl>>. Referenzen, die bereits zur Erfüllung der Mindestanforderungen herangezogen wurden (Eignungsreferenzen), dürfen nicht herangezogen werden (keine Mehrfachverwendung von Referenzen).

7.5. Zuschlagskriterien

Nur wenn die Leistungsbeschreibung und die Eignung tragfähig sind, stellt sich die Frage, ob Sicherheits- und Resilienzaspekte zusätzlich im Zuschlag bewertet werden sollen. Zuschlagskriterien können eine unklare Leistungsbeschreibung jedenfalls nicht mehr „sanieren“. Sie eignen sich nur für echte qualitative Mehrwerte, die transparent beschrieben, objektiv verglichen und nach Zuschlag vertraglich eingefordert werden können. Sicherheits- und Resilienzkonzepte können dafür geeignet sein, wenn qualitative Unterschiede tatsächlich bestehen und vorab transparent bewertet werden können. Derartige Konzepte sind dagegen ungeeignet, wenn sie bloß allgemeine Absichtserklärungen enthalten, nicht vergleichbar sind oder nach Zuschlag nicht durchgesetzt werden können.

Besondere Vorsicht ist bei der Bewertung von Reaktionsfähigkeit geboten (dazu noch später gesondert). Eine bloße Empfangsbestätigung ist in diesem Zusammenhang keine qualifizierte Reaktion. Sinnvoll ist eine gestufte Betrachtung: Erstreaktion, fachliche Triage, Remote-Bearbeitung, Vor-Ort-Einsatz, Workaround, Wiederherstellung und Abschlussbehebung. Bewertet werden dürfen nur Zusagen, die organisatorisch abgesichert, überprüfbar und vertraglich verbindlich sind.

Muster: Sicherheits- und Resilienzkonzept

Das folgende Muster eignet sich nur, wenn der Auftraggeber die geforderten Konzeptinhalte tatsächlich vergleichen und die angebotenen Mehrwerte später vertraglich einfordern kann. Es sollte daher nicht als Standardkriterium für jedes Risikoprojekt verwendet werden, sondern nur dort, wo die Konzeptqualität für die Leistungserbringung relevant ist.

Der Bieter hat ein Sicherheits- und Resilienzkonzept für die Leistungserbringung vorzulegen. Das Konzept ist Bestandteil des Angebots und wird im Zuschlag bewertet. Mindestanforderungen an die Leistung bleiben davon unberührt. Bewertet werden ausschließlich über die Mindestanforderungen hinausgehende qualitative Mehrwerte, die für die konkrete Leistungserbringung relevant, plausibel, überprüfbar und vertraglich umsetzbar sind.

Das Konzept hat folgende Themen zu behandeln:

a) Rollen, Verantwortlichkeiten und Eskalationswege,

b) Erkennung, Meldung und Behandlung von Störungen und Sicherheitsvorfällen,

c) Maßnahmen zur Sicherstellung der Verfügbarkeit und Wiederherstellung der Leistung,

d) Umgang mit Subunternehmern und Lieferkettenrisiken,

e) Personaldisposition, Schlüsselpersonen und Vertretungsregelungen,

f) Dokumentation, Nachvollziehbarkeit und Reporting,

g) Schnittstellen zum Auftraggeber,

h) Maßnahmen zur kontinuierlichen Verbesserung während der Vertragslaufzeit.

Die Bewertung erfolgt anhand folgender Kriterien:

a) Plausibilität und Auftragsbezug des Konzepts,

b) Klarheit der Verantwortlichkeiten und Eskalationswege,

c) Wirksamkeit der vorgeschlagenen Maßnahmen im Störungs- oder Sicherheitsvorfall,

d) Nachvollziehbarkeit der Dokumentation und Überprüfbarkeit der Umsetzung,

e) Qualität der Subunternehmer- und Lieferkettensteuerung,

f) Realistische Umsetzbarkeit im konkreten Leistungsumfeld.

Allgemeine, austauschbare oder nicht auf den Auftrag bezogene Ausführungen werden nicht oder nur gering bewertet. Zusagen des Bieters im Konzept werden Bestandteil des Vertrages.

Muster: Reaktionsfähigkeit bei Störungen

Die Bewertung bloßer „Reaktionszeiten“ ist in der Praxis heikel. Eine „Reaktion“ darf nicht bloß bedeuten, dass der Auftragnehmer den Eingang einer E-Mail bestätigt. Sinnvoller ist eine abgestufte Definition.

Als Reaktion gilt nicht die bloße Empfangsbestätigung einer Meldung. Bewertungsrelevant sind ausschließlich verbindlich zugesagte und organisatorisch abgesicherte Reaktionsschritte. Es wird zwischen folgenden Stufen unterschieden:

a) Erstreaktion: qualifizierte Rückmeldung durch eine fachkundige Person mit Bestätigung der Störungsannahme und erster Einschätzung,

b) Triage: fachliche Einordnung der Störung, Priorisierung und Festlegung der nächsten Schritte,

c) Remote-Bearbeitung: Beginn einer fachlichen Analyse oder Behebung aus der Ferne,

d) *Vor-Ort-Einsatz: Eintreffen qualifizierten Personals am Einsatzort, sofern erforderlich,*

e) *Workaround: Bereitstellung einer vorläufigen Ersatz- oder Umgehungslösung,*

f) *Wiederherstellung: Wiederherstellung der vereinbarten Mindestfunktion,*

g) *Abschlussbehebung: vollständige Beseitigung der Störung und Dokumentation.*

Bewertet werden nur solche Zusagen, die der Bieter nachvollziehbar organisatorisch, personell und technisch absichern kann. Der Bieter hat darzustellen, wie die zugesagten Fristen eingehalten werden, welche Personen oder Organisationseinheiten verantwortlich sind und welche Eskalationsmechanismen vorgesehen sind.

Beispiel Bewertung:

Zuschlagskriterium	**Punkte**
Qualifizierte Erstreaktion binnen *<<h>>* Stunden	*<<Punkte>>*
Remote-Triage binnen *<<h>>* Stunden	*<<Punkte>>*
Vor-Ort-Einsatz binnen *<<h>>* Stunden bei Priorität 1	*<<Punkte>>*
Bereitstellung eines Workarounds binnen *<<h>>* Stunden bei Priorität 1	*<<Punkte>>*

Grundsätzlich gilt immer zu beachten, dass bewertete Zuschlagskriterien auch die vertragliche Verknüpfung benötigen. Was zugesagt, gefordert und/oder bewertet wurde, muss im Vertrag so verankert sein, dass es während der Laufzeit tatsächlich umgesetzt, geprüft und bei Bedarf durchgesetzt werden kann.

7.6. Leistungsvertrag

Der Vertrag operationalisiert die in der Ausschreibung definierten Sicherheits- und Resilienzpflichten. Er muss klar regeln, was der Auftragnehmer tun muss, wann er es tun muss, wie er es nachweist, welche Mitwirkungspflichten bestehen, welche Subunternehmer eingesetzt werden dürfen, welche Personen Zutritt erhalten, welche Vorfälle zu melden sind, welche Auditrechte bestehen und welche Konsequenzen Verstöße haben.

Ohne vertragliche Umsetzung bleiben die Beschaffungsanforderungen häufig deklaratorisch und können den gesamten Vergabeprozess mit Rechtwidrigkeit behaften. Resilienz darf daher nicht bloße Bewertungsrhetorik sein, sondern muss in einklagbare, prüfbare und sanktionierbare Leistungspflichten übersetzt werden.

Die wichtigsten Vertragspunkte finden sich als vorformulierte Musterklauseln (Vertragsschablonen) in der Anlage. Es wird jedoch darauf hingewiesen, dass diese Musterklauseln lediglich vertragliche Ausgangspunkte sind. Eine einzelfallbezogene Prüfung ist auch in diesem Fall geboten bzw sind die Musterklauseln an Leistungsgegenstand, Kritikalität, Markt, Vergabeverfahren und interne Sicherheitsstandards des Auftraggebers anzupassen. Bei Hochrisikoprojekten sind sie zu vertiefen.

8. Sicherheitsinteressen und vergaberechtliche Transparenz

Grundsätzlich verpflichtet das Vergabeverfahren zu einer umfassenden Transparenz und zur Offenlegung aller relevanten Unterlagen im Vergabeprozess, um einen funktionierenden Wettbewerb und eine

Bietergleichbehandlung zu ermöglichen. Das vergaberechtliche Transparenzgebot gilt jedoch nicht absolut. Sicherheitsinteressen – wie insbesondere im Bereich von NISG 2026 bzw RKEG – können überwiegen und einer Veröffentlichung von Informationen im Vergabeprozess entgegenstehen. Gemeinsam begründen das NISG 2026 und das RKEG jedenfalls ein gesteigertes staatliches Interesse an der **Vertraulichkeit sicherheitsrelevanter Informationen.**

Vergaberecht verlangt somit Transparenz, Gleichbehandlung und Wettbewerb. Sicherheits- und Resilienzinteressen können demgegenüber verlangen, bestimmte Informationen nicht oder nur eingeschränkt offenzulegen. Dieses Spannungsverhältnis zeigt sich insbesondere bei Systemarchitekturen, Schwachstellenanalysen, Notfallplänen, Zutrittskonzepten, Sicherheitsmaßnahmen oder kritischen Betriebsabläufen.

Öffentliche Auftraggeber müssen daher zwei diametrale Anforderungen miteinander versöhnen: Transparenz für den Wettbewerb und Geheimnisschutz für sicherheitsrelevante Informationen.

Typische Konfliktfelder sind somit die Detailtiefe der Leistungsbeschreibung, die Offenlegung von internen Risikoanalysen, die Dokumentation von Sicherheitsanforderungen und der Informationszugang im Rahmen von Bieterfragen. Sicherheitsinteressen rechtfertigen jedenfalls keine pauschale Geheimhaltung. Umgekehrt zwingt das Transparenzgebot nicht zur unkontrollierten Offenlegung sensibler Sicherheitsinformationen. Erforderlich ist eine dokumentierte Abwägung. Praktisch bewährt sind funktionale statt detailtechnische Leistungsbeschreibungen, abgestufte Informationszugänge, Vertraulichkeitsvereinbarungen, geschützte Datenräume, anonymisierte Darstellungen und klar dokumentierte Entscheidungen im Vergabeakt. Die Reduktion der Transparenz findet ihre Grenzen jedenfalls dort, wo Bieter nicht mehr in der Lage sind, ein sachgerechtes Angebot zu erstellen, Eignungs-, Auswahl- oder Zuschlagsentscheidungen nicht mehr nachvollziehbar sind und/oder eine diskriminierungsfreie Teilnahme am Wettbewerb faktisch ausgeschlossen wird. Die Entscheidung über Beschränkungen des Informationszugangs ist im Vergabeakt zu dokumentieren.

Muster: Informationsklassifizierung

Der Auftraggeber klassifiziert die im Vergabeverfahren verwendeten Informationen nach ihrer Sensibilität. Allgemeine Informationen, die für die Angebotserstellung erforderlich sind und keine Sicherheitsrisiken begründen, werden allen Bietern zugänglich gemacht. Sicherheitsrelevante Detailinformationen, deren Offenlegung Risiken für Anlagen, Systeme, Betriebsprozesse oder Schutzmaßnahmen begründen kann, werden nur in jenem Umfang und unter jenen Bedingungen zugänglich gemacht, die für eine sachgerechte Angebotserstellung erforderlich sind.

Der Zugang zu besonders sensiblen Informationen kann von der Unterfertigung einer Vertraulichkeitserklärung, der Benennung zugriffsberechtigter Personen, der Nutzung eines geschützten Datenraums oder sonstigen angemessenen Schutzmaßnahmen abhängig gemacht werden.

Merke:

So viel Transparenz wie nötig, so viel Geheimnisschutz wie erforderlich. Beide Ziele müssen im Vergabeverfahren möglichst schonend zur Geltung gebracht werden.

9. Wann reicht die Basistoolbox nicht aus?

Die Basistoolbox ist für typische Risikoprojekte gedacht. Sie soll Auftraggebern ermöglichen, häufige Sicherheits- und Resilienzthemen strukturiert, verhältnismäßig und praxistauglich in Vergabeunterlagen und Verträge zu übersetzen. Gerade darin liegt ihr Nutzen: Sie schafft ein belastbares Grundgerüst, ohne jedes Beschaffungsvorhaben mit Maximalanforderungen, umfangreichen Zertifizierungen oder komplexen Zuschlagsmodellen zu überfrachten.

Ihre Grenze ist jedoch dort erreicht, wo die Beschaffung selbst Teil der kritischen Betriebsarchitektur wird. Das ist insbesondere dann der Fall, wenn ein Ausfall, eine Kompromittierung oder eine mangelhafte Leistungserbringung erhebliche Auswirkungen auf wesentliche Dienste, zentrale IT-/OT-Systeme, kritische Infrastruktur, Versorgungssicherheit oder Wiederanlauffähigkeit haben kann. In solchen Fällen genügt es nicht, allgemeine Standardbausteine zu übernehmen. Die Anforderungen müssen diesfalls auf den konkreten Leistungsgegenstand, die

tatsächlichen Schnittstellen, das Schadenspotenzial, die internen Betriebsprozesse und die regulatorische Betroffenheit des Auftraggebers zugeschnitten werden.

Eine vertiefte projektspezifische Ausarbeitung ist regelmäßig erforderlich, wenn zentrale IT-/OT-, Leit-, Steuerungs- oder Fernwirksysteme betroffen sind, Cloud- oder Rechenzentrumsleistungen für betriebsnahe oder sensible Daten beschafft werden, administrative Zugriffe auf produktive Systeme bestehen, Leistungen in Leitstellen, Schaltanlagen, Wasserwerken, Kläranlagen, Energie- oder Fernwärmeanlagen erbracht werden oder umfangreiche Subunternehmerketten, internationale Lieferketten, personenbezogene Zuverlässigkeitsüberprüfungen oder besonders anspruchsvolle Wiederanlaufanforderungen vorliegen.

In diesen Fällen ist eine maßgeschneiderte Lösung erforderlich. Fachbereich, Einkauf, Recht, IT-/OT-Security, Datenschutz, Betrieb, Technik und Compliance sollten gemeinsam festlegen, welche Anforderungen in der Leistungsbeschreibung, in der Eignung, im Zuschlag und im Leistungsvertrag abzubilden sind. Die Basistoolbox bleibt auch dann nützlich, weil sie die wesentlichen Themen sichtbar macht und eine gemeinsame Ausgangsbasis schafft. Sie ersetzt aber nicht die vertiefte Prüfung, welche Risiken im konkreten Projekt bestehen und wie diese vergaberechtlich, technisch, organisatorisch und vertraglich beherrscht werden können.

Schlussbemerkung: Resilienzorientierte Beschaffung bedeutet nicht, jedes Verfahren mit denselben Anforderungen zu versehen. Sie bedeutet, die Kritikalität der Beschaffung richtig einzuschätzen, die passenden Instrumente auszuwählen und Sicherheits- sowie Resilienzanforderungen dort zu verankern, wo sie ihre Wirkung entfalten. Die Basistoolbox ist dafür ein Einstieg und ein erstes Sicherungsnetz. Bei gewöhnlichen Risikoprojekten kann sie bereits einen wesentlichen Beitrag zur Absicherung leisten. Bei Hochrisikoprojekten zeigt sie, an welchen Stellen der Standard endet und die detailliertere Ausarbeitung „nach Maß“ beginnen muss.

Anlage „Musterklauseln“

Muster: Basisklausel Sicherheits- und Resilienzanforderungen

Der Auftragnehmer hat die Leistung so zu erbringen, dass die Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit und Nachvollziehbarkeit der vom Auftrag betroffenen Systeme, Anlagen, Informationen und Betriebsprozesse angemessen gewahrt bleiben.

Der Auftragnehmer hat insbesondere die für die Leistungserbringung relevanten Sicherheits- und Zutrittsvorgaben des Auftraggebers einzuhalten, sicherheits- oder betriebsrelevante Störungen unverzüglich zu melden, eingesetztes Personal vor Leistungsbeginn zu unterweisen, Subunternehmer nur nach Maßgabe der Ausschreibungs- und Vertragsbestimmungen einzusetzen, sicherheitsrelevante Tätigkeiten nachvollziehbar zu dokumentieren, an Analyse und Behebung von Störungen mitzuwirken, vertrauliche Informationen zu schützen und den Auftraggeber bei gesetzlichen Auskunfts-, Nachweis- und Meldepflichten angemessen zu unterstützen.

Muster: Vertraulichkeit

Der Auftragnehmer verpflichtet sich, sämtliche ihm im Zusammenhang mit dem Vergabeverfahren, dem Vertrag und der Leistungserbringung bekannt werdenden Informationen über Anlagen, Systeme, Betriebsabläufe, Sicherheitsmaßnahmen, Schwachstellen, Notfallprozesse, Zutrittsregelungen, technische Schnittstellen, Betriebsdaten und Schutzkonzepte des Auftraggebers streng vertraulich zu behandeln.

Die Vertraulichkeit gilt auch dann, wenn eine Information nicht ausdrücklich als vertraulich bezeichnet wurde, ihre Schutzwürdigkeit sich aber aus Inhalt, Zusammenhang oder Umständen ergibt. Der Auftragnehmer darf vertrauliche Informationen nur zur Vertragserfüllung verwenden und nur jenen Personen zugänglich machen, die sie hierfür benötigen. Diese Pflicht ist allen eingesetzten Mitarbeitenden und Subunternehmern nachweislich zu überbinden.

Muster: Incident-Meldung

Der Auftragnehmer hat Sicherheitsvorfälle, Betriebsstörungen, Schwachstellen, unberechtigte Zugriffe, Datenverluste, Systemausfälle, Fehlfunktionen, Manipulationsverdacht, Verlust von Zutrittsmitteln oder sonstige

Ereignisse, die Sicherheit, Verfügbarkeit, Integrität, Vertraulichkeit oder Wiederanlauffähigkeit beeinträchtigen oder beeinträchtigen können, unverzüglich nach Kenntnis an den Auftraggeber zu melden.

Die Meldung hat, soweit bekannt, Art und Zeitpunkt des Vorfalls, betroffene Leistungen, Systeme, Anlagen, Daten oder Prozesse, vermutete Ursache, mögliche Auswirkungen, bereits gesetzte Sofortmaßnahmen, empfohlene weitere Maßnahmen, zuständige Ansprechperson und voraussichtliche Dauer bis zur nächsten qualifizierten Rückmeldung zu enthalten.

Muster: Subunternehmer für sensible Leistungsteile

Der Einsatz von Subunternehmern bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers. Der Auftragnehmer hat vor Einsatz des Subunternehmers dessen Identität, Leistungsumfang, betroffene Schnittstellen, Standorte, Systeme oder Anlagen sowie die vorgesehenen Sicherheits-, Vertraulichkeits- und Kontrollmaßnahmen bekanntzugeben.

Der Auftragnehmer hat sicherzustellen, dass sämtliche Sicherheits-, Resilienz-, Vertraulichkeits-, Melde-, Mitwirkungs-, Audit-, Zutritts-, Dokumentations- und Personalpflichten auch vom Subunternehmer eingehalten werden. Der Auftragnehmer haftet für Subunternehmer wie für eigenes Verhalten.

Muster: Zutritt und Ausweise

Der Auftragnehmer darf Betriebsstätten, Anlagen, Baustellen, Leitstellen, Rechenzentren, Serverräume, technische Betriebsräume oder sonstige sicherheitsrelevante Bereiche des Auftraggebers nur mit vorab bekanntgegebenem und zutrittsberechtigtem Personal betreten.

Zutrittsmittel, Ausweise, Schlüssel, Zugangskarten, Codes, Token oder sonstige Berechtigungen sind sorgfältig zu verwahren, dürfen nicht an Dritte weitergegeben werden und sind nach Beendigung des Einsatzes oder auf Verlangen unverzüglich zurückzugeben. Verlust, Diebstahl oder Missbrauchsverdacht sind unverzüglich zu melden.

Muster: Sicherheitsunterweisung

Der Auftragnehmer hat sicherzustellen, dass sämtliche eingesetzten Personen vor Aufnahme ihrer Tätigkeit über die für die Leistungserbringung relevanten Sicherheits-, Vertraulichkeits-, Zutritts-, Melde-, Datenschutz- und Verhaltenspflichten unterwiesen werden.

Die Unterweisung ist zu dokumentieren und dem Auftraggeber auf Verlangen nachzuweisen. Ohne vorherige Unterweisung dürfen Personen in sicherheitsrelevanten Bereichen nicht eingesetzt werden.

Muster: Fehlermanagement

Der Auftragnehmer hat ein strukturiertes Fehlermanagement einzurichten und während der Vertragslaufzeit aufrechtzuerhalten. Fehler, Mängel, Störungen und Abweichungen sind nach Schweregrad zu klassifizieren, nachvollziehbar zu dokumentieren, innerhalb der vereinbarten Fristen zu analysieren und zu beheben.

Bei wiederkehrenden oder sicherheitsrelevanten Fehlern hat der Auftragnehmer eine Ursachenanalyse durchzuführen und dem Auftraggeber geeignete Korrektur- und Präventionsmaßnahmen vorzuschlagen. Der Auftragnehmer hat auf Verlangen Auskunft über Fehlerursache, Auswirkungen, gesetzte Maßnahmen, verbleibende Risiken und geplante Abhilfemaßnahmen zu erteilen.

Muster: Incident Management

Der Auftragnehmer hat für sicherheits- oder betriebsrelevante Vorfälle ein angemessenes Incident Management vorzuhalten. Dieses hat jedenfalls Prozesse zur Erkennung, Meldung, Eskalation, Analyse, Eindämmung, Behebung, Dokumentation und Nachbereitung von Vorfällen zu umfassen.

Der Auftragnehmer hat dem Auftraggeber geeignete Ansprechpersonen, Erreichbarkeiten und Eskalationswege bekanntzugeben. Änderungen sind unverzüglich mitzuteilen. Nach Abschluss eines erheblichen Vorfalls hat der Auftragnehmer auf Verlangen einen Vorfallsbericht zu erstellen, der Ursache, Verlauf, Auswirkungen, gesetzte Maßnahmen, verbleibende Risiken und empfohlene Präventionsmaßnahmen darstellt.

Muster: Logging und Nachvollziehbarkeit

Der Auftragnehmer hat sicherzustellen, dass sicherheits- und betriebsrelevante Zugriffe, Änderungen, Administrationshandlungen, Konfigurationsänderungen, Störungen und sonstige relevante Ereignisse angemessen protokolliert werden, soweit dies für die vertragsgegenständliche Leistung erforderlich und rechtlich zulässig ist.

Die Protokolle müssen eine nachträgliche Nachvollziehbarkeit wesentlicher Vorgänge ermöglichen und sind vor unberechtigter Veränderung und unberechtigtem Zugriff zu schützen. Der Auftraggeber erhält im Anlassfall Einsicht in jene Protokolle oder Auswertungen, die zur Aufklärung von Störungen, Sicherheitsvorfällen, Vertragsverletzungen oder behördlichen Auskunfts- und Nachweispflichten erforderlich sind.

Logging-, Monitoring- und Kontrollmaßnahmen sind verhältnismäßig auszugestalten. Insbesondere ist festzulegen, welche Ereignisse protokolliert werden, wer Zugriff auf Protokolle erhält, wie lange Protokolle aufbewahrt werden und in welchen Anlassfällen eine Auswertung zulässig ist.

Muster: Berechtigungs- und Rollenkonzept

Der Auftragnehmer hat für die Leistungserbringung ein angemessenes Berechtigungs- und Rollenkonzept vorzusehen. Zugriffs-, Zutritts- und Administrationsrechte sind auf das für die jeweilige Tätigkeit erforderliche Ausmaß zu beschränken. Administrative oder besonders privilegierte Rechte dürfen nur Personen eingeräumt werden, die diese Rechte für die Erfüllung ihrer Aufgaben benötigen.

Berechtigungen sind regelmäßig zu überprüfen und nicht mehr erforderliche Berechtigungen unverzüglich zu entziehen. Änderungen von Berechtigungen sind nachvollziehbar zu dokumentieren. Zugangsdaten, Schlüssel, Karten, Token und vergleichbare Berechtigungsmittel dürfen nicht unbefugt weitergegeben oder gemeinsam genutzt werden.

Muster: Ersatzteil- und Personalverfügbarkeit

Der Auftragnehmer hat während der Vertragslaufzeit sicherzustellen, dass die zur ordnungsgemäßen Leistungserbringung erforderlichen personellen Ressourcen, Ersatzteile, Komponenten, Werkzeuge, Lizenzen, Dokumentationen und sonstigen Betriebsmittel in angemessener Frist verfügbar sind.

Für kritische Leistungsteile hat der Auftragnehmer geeignete Vorkehrungen zur Vermeidung von Lieferverzögerungen, Schlüsselpersonenabhängigkeiten und Wiederanlaufhindernissen zu treffen. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn absehbar ist, dass wesentliche Ressourcen nicht rechtzeitig verfügbar sein werden.

Muster: Auditrechte

Der Auftraggeber ist berechtigt, die Einhaltung der vereinbarten Sicherheits-, Vertraulichkeits-, Resilienz-, Subunternehmer-, Personal-, Zutritts-, Dokumentations- und Meldepflichten in angemessenem Umfang selbst oder durch geeignete Dritte überprüfen zu lassen.

Der Auftragnehmer hat an solchen Prüfungen mitzuwirken, erforderliche Unterlagen bereitzustellen und Zugang zu relevanten Informationen zu gewähren, soweit dies zur Überprüfung der vertraglichen Pflichten erforderlich und verhältnismäßig ist. Audits sind, soweit keine Gefahr im Verzug besteht, mit angemessener Frist anzukündigen und so durchzuführen, dass der Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigt wird.

Muster: Exitmanagement

Der Auftragnehmer hat bei Vertragsbeendigung, Vertragsablauf, Kündigung oder Wechsel des Leistungserbringers an einer geordneten Übergabe mitzuwirken. Er hat insbesondere jene Informationen, Dokumentationen, Zugangsdaten, Konfigurationen, Schnittstellenbeschreibungen, Bestandsdaten, Protokolle und sonstigen Übergabeunterlagen vollständig, aktuell und in einem nutzbaren Format bereitzustellen, die für die Fortführung oder Übernahme der Leistung erforderlich sind.

Der Auftragnehmer hat den Auftraggeber und einen allfälligen Nachfolgeauftragnehmer in angemessenem Umfang zu unterstützen. Vertraulichkeits-, Datenschutz-, Sicherheits- und Mitwirkungspflichten bleiben bis zum Abschluss der Übergabe aufrecht.

Muster: Mitwirkung bei behördlichen Auskunfts-, Prüf- und Meldepflichten

Der Auftragnehmer hat den Auftraggeber bei behördlichen Auskunfts-, Prüf-, Nachweis- und Meldepflichten angemessen zu unterstützen, soweit diese mit der vertragsgegenständlichen Leistung zusammenhängen. Dies umfasst insbesondere die zeitgerechte Bereitstellung von Informationen, technischen Beschreibungen, Dokumentationen, Vorfallsberichten, Nachweisen über gesetzte Maßnahmen, Protokollen, Auditunterlagen und sonstigen sachdienlichen Informationen.

Die Mitwirkung hat unverzüglich, vollständig und in strukturierter Form zu erfolgen. Vertrauliche oder personenbezogene Informationen sind nur im erforderlichen und rechtlich zulässigen Umfang bereitzustellen.

Muster: Post-Incident-Review

Nach erheblichen Sicherheits- oder Betriebsvorfällen hat der Auftragnehmer auf Verlangen des Auftraggebers an einer strukturierten Nachbereitung mitzuwirken. Ziel der Nachbereitung ist es, Ursachen, Auswirkungen, Reaktionszeiten, Wirksamkeit gesetzter Maßnahmen und Verbesserungsmöglichkeiten festzustellen.

Die Ergebnisse sind in einem kurzen Bericht zusammenzufassen. Der Auftragnehmer hat angemessene Korrektur- und Präventionsmaßnahmen vorzuschlagen und jene Erkenntnisse, die seinen Verantwortungsbereich betreffen, in seine Prozesse, Schulungen und Dokumentationen einfließen zu lassen.

Muster: Vertragsstrafe und außerordentliche Kündigung

Verstöße gegen wesentliche Sicherheits-, Vertraulichkeits-, Melde-, Zutritts-, Subunternehmer-, Personal-, Audit- oder Mitwirkungspflichten stellen eine wesentliche Vertragsverletzung dar. Der Auftraggeber wird dem Auftragnehmer eine angemessene Frist zur Herstellung des vertragskonformen Zustands setzen, sofern nicht Gefahr im Verzug besteht oder die Vertragsverletzung ihrer Art nach nicht behebbar ist.

Bei Verstößen ist der Auftraggeber zur außerordentlichen Kündigung aus wichtigem Grund berechtigt. Für schuldhafte Verstöße hat der Auftragnehmer eine Vertragsstrafe in Höhe von EUR <<Betrag>> je Einzelfall zu leisten. Die Geltendmachung eines darüber hinausgehenden Schadens bleibt unberührt.